What is claimed is:

1. A method of detecting unauthorized access attempts to a network, the method comprising:

receiving a request from a user to obtain an address;

obtaining said address;

applying a function to said address to obtain a return address, said return address corresponding to a used one of a block of addresses;

returning said return address to said user;

monitoring access to said address; and

detecting an unauthorized attempt to access said address when an attempted address corresponds to an unused one of said block of addresses.

2. A method according to claim 1, wherein applying said function comprises hashing a user address of said user to obtain one value of a range of values mapping to said block of addresses, said one value designating said used one of said block of addresses.

3. A method according to claim 2, wherein applying said function comprises hashing a time of said request.

4. A method according to claim 2, wherein detecting comprises tracing said user when said attempted address corresponds to said unused one of said block of addresses.

5. A method according to claim 4, comprising blocking additional unauthorized attempts when said attempted address corresponds to said unused one of said block of addresses.

6. A method according to claim 4, wherein unused ones of said block of addresses correspond to attack detectors.

7. A method according to claim 1, wherein said function comprises hashing a time of said request to obtain one value of a range of values mapping to said block of addresses, said one value designating said used one of said block of addresses.

8. A method according to claim 1, wherein applying said function comprises changing said used one of said block of addresses over time.

9. A method according to claim 8, wherein applying said function comprises determining a time period for changing said one of said block of addresses.

10. A method according to claim 9, wherein determining a time period comprises using a pre-selected time period.

11. A method according to claim 9, wherein determining a time period comprises generating a random time period.

12. A method according to claim 8, wherein changing said used one of said block of addresses comprises randomly choosing said used one from said block of addresses.

13. A method according to claim 8, wherein detecting comprises tracing said user when said attempted address corresponds to said unused one of said block of addresses.

14. A method according to claim 13, comprising blocking additional unauthorized attempts when said attempted address corresponds to said unused one of said block of addresses.

15. A method according to claim 13, wherein unused ones of said block of addresses correspond to attack detectors.

16. A method according to claim 8, further comprising determining said attempt is authorized when a connection exists between said user and said unused address.

17. A method according to claim 8, wherein changing said used one of said block of addresses comprises coordinating changes in a name-to-address database and a host identity-to-address database.

18. A method according to claim 1, wherein detecting comprises tracing said user when said attempted address corresponds to said unused one of said block of addresses.

19. A method according to claim 18, comprising blocking additional unauthorized attempts when said attempted address corresponds to said unused one of said block of addresses.

20. A method according to claim 1, wherein unused ones of said block of addresses correspond to attack detectors.

21. A computer-readable medium containing instructions for controlling a processor to detect unauthorized access attempts to a network by:

receiving a request from a user to obtain an address;

obtaining said address;

applying a function to said address to obtain a return address, said return address corresponding to a used one of a block of addresses;

returning said return address to said user;

monitoring access to said address; and

detecting an unauthorized attempt to access said address when an attempted address corresponds to an unused one of said block of addresses.

22. The computer-readable medium of claim 21, further comprising instructions for controlling a processor to apply said function by hashing at least one of a user address of said user and a time of said request to obtain one value of a range of values mapping to said block of addresses, said one value designating said used one of said block of addresses.

23. The computer-readable medium of claim 21, further comprising instructions for controlling a processor to detect said unauthorized attempt by tracing said user when said attempted address corresponds to said unused one of said block of addresses.

24. The computer-readable medium of claim 23, further comprising instructions for controlling a processor to detect said unauthorized attempt by blocking additional unauthorized attempts when said attempted address corresponds to said unused one of said block of addresses.

25. The computer-readable medium of claim 21, further comprising instructions for controlling a processor to apply said function by changing said used one of said block of addresses over time.

26. The computer-readable medium of claim 25, further comprising instructions for controlling a processor to change said used one of said block of addresses over time by at least one of determining a time period using a pre-selected time period and determining a time period by generating a random time period.

27. The computer-readable medium of claim 25, further comprising instructions for controlling

a processor to change said used one of said block of addresses by randomly choosing said used one from said block of addresses.

28. The computer-readable medium of claim 25, further comprising instructions for controlling a processor to determine said attempt is authorized by determining that a connection exists between said user and said unused address.

29. The computer-readable medium of claim 25, further comprising instructions for controlling a processor to change said used one of said block of addresses by coordinating changes in a name-to-address database and a host identity-to-address database.

30. A system for detecting unauthorized access attempts to a network, the system comprising:

means for receiving a request from a user to obtain an address;

means for obtaining said address;

means for applying a function to said address to obtain a return address, said return address corresponding to a used one of a block of addresses;

means for returning said return address to said user;

means for monitoring access to said address; and

means for detecting an unauthorized attempt to access said address when an attempted address corresponds to an unused one of said block of addresses.

31. The system of claim 30, wherein said means for applying further comprises means for hashing at least one of a user address of said user and a time of said request to obtain one value of a range of values mapping to said block of addresses, said one value designating said used one of said block of addresses.

32. The system of claim 30, wherein said means for detecting further comprise means for tracing

said user when said attempted address corresponds to said unused one of said block of addresses.

33. The system of claim 32, wherein said means for detecting further comprise means for blocking additional unauthorized attempts when said attempted address corresponds to said unused one of said block of addresses.

34. The system of claim 30, wherein said means for applying further comprise means for changing said used one of said block of addresses over time.

35. The system of claim 34, wherein said means for changing further comprise at least one of means for determining a time period using a pre-selected time period and means for determining a time period by generating a random time period.

36. The system of claim 34, wherein said means for changing further comprise means for randomly choosing said used one from said block of addresses.

37. The system of claim 34, further comprising means for determining said attempt is authorized when a connection exists between said user and said unused address.

38. The system of claim 34, further comprising:

a name-to-address database;

a host identity-to-address database; and

means for coordinating changes in said name-to-address database and said host identity-to-address database in conjunction with said means for changing.

39. A computer program, disposed on a computer-readable medium, for enabling detection of

unauthorized access attempts to a network, said computer program including instructions for causing a processor to:

receive a request from a user to obtain an address;

obtain said address;

apply a function to said address to obtain a return address, said return address corresponding to a used one of a block of addresses;

return said return address to said user;

monitor access to said address; and

detect an unauthorized attempt to access said address when an attempted address corresponds to an unused one of said block of addresses.

40. The computer program of claim 39, wherein said instructions for causing a processor to apply said function further include instructions for causing a processor to at least one of hash a user address of said user and hash a time of said request to obtain one value of a range of values mapping to said block of addresses, said one value designating said used one of said block of addresses.

41. The computer program of claim 40, wherein said instructions for causing a processor to detect further include instructions for causing a processor to trace said user when said attempted address corresponds to said unused one of said block of addresses.

42. The computer program of claim 41, further including instructions for causing a processor to block additional unauthorized attempts when said attempted address corresponds to said unused one of said block of addresses.

43. The computer program of claim 41, further including instructions for causing a processor to correspond said unused ones of said block of addresses with attack detectors.

44. The computer program of claim 39, wherein said instructions for causing a processor to apply said function further include instructions for causing a processor to change said used one of said block of addresses over time.

45. The computer program of claim 44, wherein said instructions for causing a processor to apply said function further include instructions for causing a processor to at least one of use a pre-selected time period for changing said one of said block of addresses and generate a random time period for changing said one of said block of addresses.

46. The computer program of claim 44, wherein said instructions for causing a processor to change said used one of said block of addresses further include instructions for causing a processor to randomly choose said used one from said block of addresses.

47. The computer program of claim 44, wherein said instructions for causing a processor to detect further include instruction for causing a processor to trace said user when said attempted address corresponds to said unused one of said block of addresses.

48. The computer program of claim 47, further including instructions for causing a processor to block additional unauthorized attempts when said attempted address corresponds to said unused one of said block of addresses.

49. The computer program of claim 47, further including instructions for causing a processor to correspond attack detectors with unused ones of said block of addresses.

50. The computer program of claim 44, further including instructions for causing a processor to determine said attempt is authorized when a connection exists between said user and said unused

address.

51. The computer program of claim 44, further including instructions for causing a processor to coordinate said change in a name-to-address database and a host identity-to-address database.

52. The computer program of 39, wherein said instructions for causing a processor to detect further include instructions for causing a processor to trace said user when said attempted address corresponds to said unused one of said block of addresses.

53. The computer program of claim 52, further including instructions for causing a processor to block additional unauthorized attempts when said attempted address corresponds to said unused one of said block of addresses.

54. The computer program of claim 39, further including instructions for causing a processor to correspond attack detectors with unused ones of said block of addresses.